ESET®

SECURITY
FOR MICROSOFT SHAREPOINT SERVER

Protect sensitive data in Microsoft SharePoint, using multilayered technology

Progress. Protected.

What is a **SharePoint security solution?**

A SharePoint security product is designed to protect the central collaboration servers of an organization from threats. This product should be installed on any SharePoint server in an organization to ensure that resources are not infected. Companies nowadays put their organization at risk by allowing users to save and upload files to a company SharePoint, without adequately protecting their SharePoint from malicious files. A single user uploading a malicious file to SharePoint can instantly cause a cascade effect that renders your organization's files inaccessible.

ESET Security for Microsoft Sharepoint provides advanced protection to all SharePoint servers to protect against malicious uploads and unwanted files. It pays special attention to ensure the servers are stable and conflict-free in order to minimize maintenance windows and restarts, so that business continuity is not disrupted.

The ESET Difference

MULTILAYERED PROTECTION

ESET combines multilayered technology, machine learning and human expertise to provide our customers with the best level of protection possible. Our technology is constantly adjusting and changing to provide the best balance of detection, false positives and performance.

DIRECT DATABASE ACCESS

An optional method to pull file, where ESET SharePoint Security bypasses the SharePoint object model and pulls the file directly from the dedicated database server to provide even better performance.

UNPARALLELED PERFORMANCE

Countless times, an organization's biggest concern is the performance impact of an endpoint protection solution. ESET products continue to excel in the performance arena and win third-party tests that prove how light their impact is on users' systems.

WORLDWIDE PRESENCE

ESET has offices in 22 countries worldwide, R&D labs in 13 and a presence in over 200 countries and territories. This helps to provide us with data to stop malware prior to it spreading across the globe, as well as prioritize new technologies based on the most recent threats or possible new vectors.

REMOTE MANAGEMENT

All ESET endpoint solutions are managed from our single-pane-of-glass cloud console, ESET PROTECT, ensuring a complete overview of your network. This delivers real-time visibility for on-premise and off-premise endpoints, as well as full reporting and security management for all operating systems.

★★★★★

"...THE BEST TESTIMONY? THE STATS FROM OUR HELPDESK: AFTER WE INTRODUCED ESET, OUR SUPPORT GUYS DON'T LOG ANY CALLS – THEY DON'T HAVE TO DEAL WITH ANY ANTIVIRUS OR MALWARE-RELATED ISSUES!"

Adam Hoffman, IT Infrastructure Manager;
Mercury Engineering, Ireland; 1.300 seats

Our unique, multilayered approach to security

ESET LiveSense technology, combined with our machine learning expertise, cloud reputation system, and our people, together power the world's most formidable cyber threat prevention, detection and response platform.

ESET LIVEGRID®

Whenever a zero-day threat such as ransomware is seen, the file is sent to our cloud-based malware protection system, LiveGrid®, where the threat is detonated and its behavior is monitored. The results of this system are provided to all endpoints globally within minutes without requiring any updates.
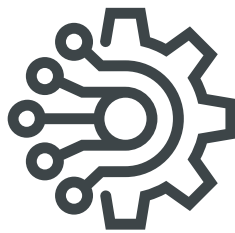
MACHINE LEARNING

Uses the combined power of neural networks and handpicked algorithms to correctly label incoming samples as clean, potentially unwanted or malicious.

HUMAN EXPERTISE

ESET's world-class security researchers share elite know-how and intelligence to ensure our users benefit from optimum, round-the-clock threat intelligence.

BRUTE FORCE ATTACK PROTECTION

A security feature that protects devices against potential guessing of credentials and illegitimate establishment of a remote connection. Protection can be easily configured through a policy directly from the console, and exclusions can be created when something is blocked but shouldn't be.
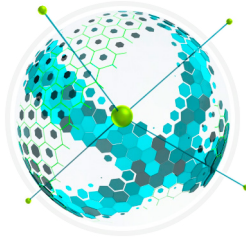
NETWORK ATTACK PROTECTION

This technology improves detection of known vulnerabilities on the network level. It constitutes another important layer of protection against the spread of malware, network-conducted attacks, and exploitation of vulnerabilities for which a patch has not yet been released or deployed.
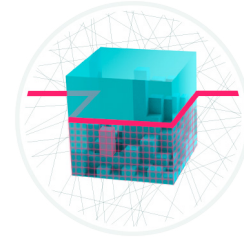
AMSI/SCRIPT SCANNING

ESET solutions leverage the Antimalware Scan Interface (AMSI) to provide enhanced malware protection for users, data, applications, and workload. In addition, it utilizes the protected service interface that is a new security module built into Windows that only allows trusted, signed code to load and better protect against code injection attacks.
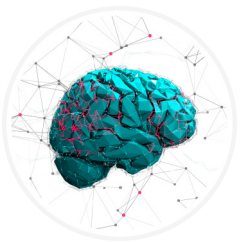
MACHINE LEARNING

All ESET endpoint products have been using machine learning in addition to all other layers of defense since 1997. ESET currently uses machine learning in conjunction with all of our other layers of defense. Specifically, machine learning is used in the form of consolidated output and neural networks.

RANSOMWARE SHIELD

ESET Ransomware Shield is an additional layer protecting users from ransomware. This technology monitors and evaluates all executed applications based on their behavior and reputation. It is designed to detect and block processes that resemble the behavior of ransomware.
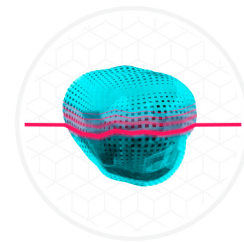
ADVANCED MEMORY SCANNER

ESET Advanced Memory Scanner monitors the behavior of a malicious process and scans it once it decloaks in memory. Fileless malware operates without needing persistent components in the file system that can be detected conventionally. Only memory scanning can successfully discover and stop such malicious attacks.

These are some of ESET LiveSense's core technologies and indicate approximately when and where they detect and block threats, covering the entire threat lifecycle in the system—from its pre-boot to resting state. Learn more

eseT ® Digital Security
Progress. Protected.
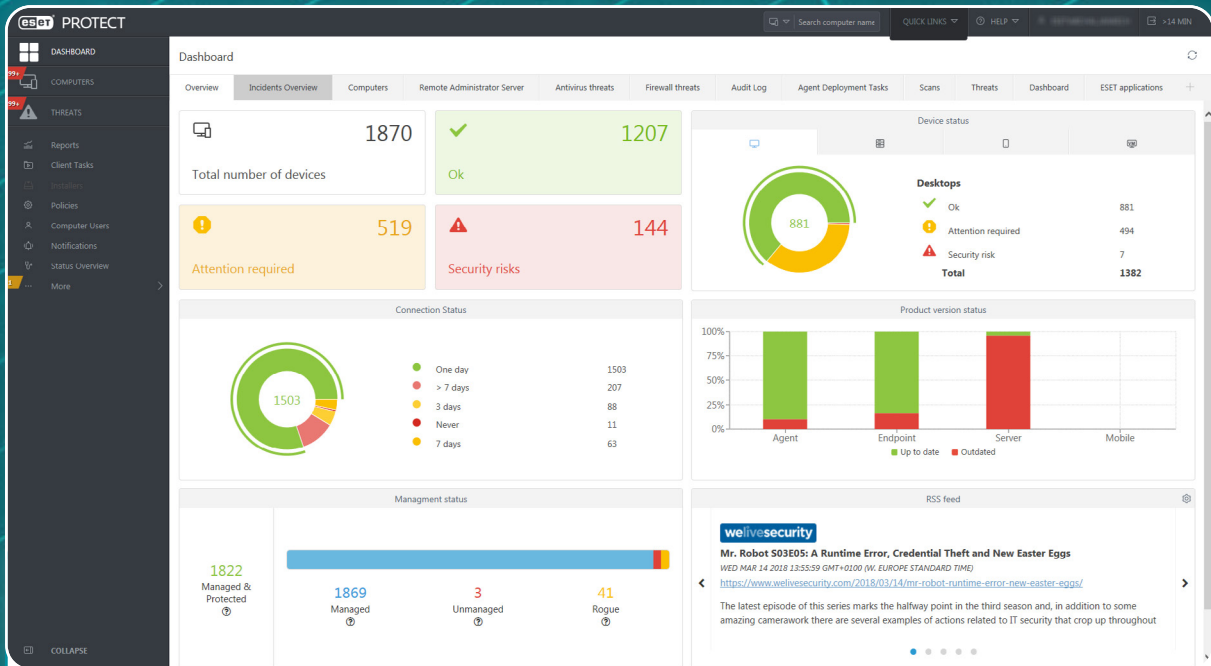
ESET PROTECT

All ESET endpoint solutions are managed from
a single-pane-of-glass cloud console, ESET PROTECT,
ensuring a complete overview of your network.

Use cases

Fileless malware

PROBLEM

File-less malware is a relatively new threat. It exists only in memory, so requires a different approach compared to traditional file-based malware.

SOLUTION

✔ A unique ESET technology, Advanced Memory Scanner, protects against this type of threat by monitoring the behavior of malicious processes and scanning them once they decloak in memory.

✔ If a threat is confirmed, reduce data gathering and investigation time by uploading it into ESET Threat intelligence to provide information on how the threat functions.

Zero-day threats

PROBLEM

Zero-day threats are a major concern for businesses due to them not knowing how to protect against something that they have never seen before.

SOLUTION

✔ ESET Threat Intelligence provides data on the newest threats and trends as well as targeted attacks to help businesses predict and prevent them.

✔ ESET endpoint products leverage heuristics and machine learning as part of our multi-layered approach to prevent and protect against never-before-seen malware.

✔ ESET's cloud malware protection system automatically protects against new threats without the need to wait for the next detection update.

Ransomware

PROBLEM

Some businesses want extra insurance that they will be protected from ransomware attacks. In addition, they want to ensure their network drives are safe from unauthorized encryption.

SOLUTION

✔ On upload of a file into the SharePoint Server, ESET scans files to ensure they are not malicious.

✔ Network Attack Protection has the ability to prevent ransomware from ever infecting a system, by stopping exploits at the network level.

✔ Our multilayered defense features an in-product sandbox that has the ability to detect malware that attempts to evade detection by using obfuscation.

✔ Leverage ESET's cloud malware protection system to automatically protect against new threats without the need to wait for the next detection update.

✔ All products contain post-execution protection in the form of Ransomware Shield to ensure that businesses are protected from malicious file encryption.

About ESET

Next-gen digital security for business

WE DON'T JUST STOP BREACHES—WE PREVENT THEM

Unlike conventional solutions that focus on reacting to threats after they've been executed, ESET offers an unmatched AI-powered prevention-first approach backed by human expertise, renowned global Threat Intelligence, and an extensive R&D network led by industry-acclaimed researchers—all for the continuous innovation of our multilayered security technology.

Experience unparalleled protection from ransomware, phishing, zero-day threats and targeted attacks with our award-winning, cloud-first XDR cybersecurity platform that combines next-gen prevention, detection, and proactive threat hunting capabilities. Our highly customizable solutions include hyperlocal support. They offer minimal impact on endpoint performance, identify and neutralize emerging threats before they can be executed, ensure business continuity, and reduce the cost of implementation and management.

In a world where technology enables progress, protect your business with ESET.

ESET IN NUMBERS

1bn+
protected internet users

400k+
business customers

200
countries and territories

13
global R&D centers

SOME OF OUR CUSTOMERS

MITSUBISHI MOTORS
Drive your Ambition

protected by ESET since 2017
more than 9,000 endpoints

Allianz Suisse

protected by ESET since 2016
more than 4,000 mailboxes

Canon
Canon Marketing Japan Group

protected by ESET since 2016
more than 32,000 endpoints

· · · ·

ISP security partner since 2008
2 million customer base

RECOGNITION

AV comparatives
APPROVED
Business Security
JUL 2023

ESET received the Business Security APPROVED award from AV - Comparatives in the Business Security Test in July 2023.

Leader
SUMMER
2023

ESET consistently achieves top rankings on the global G2 user review platform and its solutions are appreciated by customers worldwide.

THE RADICATI GROUP, INC.
A TECHNOLOGY MARKET RESEARCH FIRM

ESET has been recognized as a 'Top Player' for the fourth year in a row in Radicati's 2023 Advanced Persistent Threat Market Quadrant.